

Apache met virtual hosts op CentOS7

installeren

Installeer apache en de nodig SSL software en zorg dat apache start als de server boot:

```
yum install httpd openssl mod_ssl -y
systemctl enable httpd.service
```

firewall

Zet de nodige poorten in de firewall open zodat er van buitenaf verbinding kan worden gemaakt:

```
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

hardening

harden de httpd install door de volgende entries toe te voegen aan: vi /etc/httpd/conf.d/options.conf

```
TraceEnable off

## Disable Signature
ServerSignature Off

## Disable Banner
ServerTokens Prod
```

Virtual hosts

setup het virtual hosts systeem zodat op deze server meerdere webapplicaties geïnstalleerd kunnen worden.

Maak de directories voor de config files:

```
mkdir /etc/httpd/sites-available
mkdir /etc/httpd/sites-enabled
```

voeg de parsing hiervan toe aan de configuratie: vi /etc/httpd/conf/httpd.conf en voeg hierin toe:

```
IncludeOptional sites-enabled/*.conf
```

Vervolgens kan later de configuratie file voor een virtual host worden gemaakt. Je maakt dan de conf file in sites-available, en zodra je in de lucht wil leg je een link naar die file in sites-enabled door:

```
ln -s /etc/httpd/sites-available/name-of-site.conf /etc/httpd/sites-enabled/name-of-site.conf
```

SSL certificaten

in principe maak je per virtual webhost een certificaat/key pair aan en distribueer je die ook naar de reverse proxy.

maak de sefsigned SSL certificaten
cd /etc/ssl

maak de server key:
openssl genrsa -des3 -out server.key 1024

Er zit verplicht een passphrase op de key. Die moet er af anders moet je die elke keer opgeven als apache start, dit betekent dat de server niet autonoom kan opstarten. haal je hem er als volgt af:
cp server.key server.key.org
openssl rsa -in server.key.org -out server.key

maak een certificate signing request:
openssl req -new -key server.key -out server.csr

en vul alles in

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

```
-----
```

```
Country Name (2 letter code) [XX]:NL
State or Province Name (full name) []:Zuid Holland
Locality Name (eg, city) [Default City]:Den Haag
Organization Name (eg, company) [Default Company Ltd]:Boerema CI&ND
Organizational Unit Name (eg, section) []:IT Dept.
Common Name (eg, your name or your server's hostname) []:wiki.auriel.nl
Email Address []:webmaster@auriel.nl
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

maak het selfsigned certificaat aan:
openssl x509 -req -days 3650 -in server.csr -signkey server.key -out

server.crt

en kopieer de certificaten naar de apache configuratie:

```
cp server.crt /usr/local/apache/conf/ssl.crt
```

```
cp server.key /usr/local/apache/conf/ssl.key
```

start de web server door:

```
systemctl start httpd.service
```

From:

<https://wiki.auriel.nl/> -

Permanent link:

https://wiki.auriel.nl/doku.php?id=installatie_handleidingen:apache&rev=1448880655 

Last update: **2015/11/30 11:50**